2010 Information Technology Governance Report (ITGR) Frequently Asked Questions (FAQ)

Formerly AISR (Agency Information Security Report)

General Information, Process and System Access

Q: Does my agency have to report and why do we have to do it every year?

A: Governor Perdue's executive order (EO) requires annual reporting by all Executive Branch agencies. All other agencies are required (based on AG interpretation of GA code) to adhere to security standards published by GTA and are strongly encouraged to follow the executive order. In 2009, Legislation updated GTA power to publish an annual state information technology report and authorized GTA to solicit reporting data from agencies up to twice a year.

Each year, state leaders must make important decisions regarding strategic goals and objectives for the coming year. The annual report is a tool to help facilitate informed decision making in support of those goals. It provides a uniform method to regularly measure the health of information technology matters that affect how the state manages the IT services it provides and the information entrusted to its care.

The report can also demonstrate quantifiable progress in accomplishing strategic goals by identifying areas that require more focus as well as highlighting those areas exemplifying being the best managed state.

Q: What is the deadline for submitting my agency's ITGR?

A: ITGR timeline and deliverables (all dates are for year 2010):

March 31	GTA publishes the IT Reporting Standard for that year
NLT June 15	GTA makes ITGR system available to agencies to complete their ITGR online. (The goal is to make ITGR system available year-round for agencies to maintain and update their information as necessary rather than waiting for June of each year.)
July 31	Completed and Approved ITGR due to GTA
Oct 1	GTA publishes annual State IT Report
NLT Oct 31	GTA publishes annual Enterprise Information Security Report

Q: What time period does the report cover?

A: As per the Governor's Executive Order and the IT Reporting standard, each agency shall report on the status of their agency's information technology program as of June 30th of each year. This means that the report should pertain to the current fiscal year. For example, in 2010, the reporting period will cover FY 2010 (July 1, 2009 to June 30, 2010).

Q: What is the consequence to my agency if we aren't able to show progress from the 2009 Plan of Actions and Milestones?

A: The ITGR is intended to assess and continually improve the security, reliability and effectiveness of information technology from a Statewide Enterprise perspective. To accomplish that goal, each agency must report and while it is understandable that some agencies are further along on the maturity scale than others, the ITGR is NOT intended to "punish" agencies that still have work to do in these areas. Instead it is intended to be a tool to highlight areas for improvement and facilitate management decisions that will help the agencies and ultimately the state continue to progress up the maturity scale.

Q: When will the ITGR system be available and how do I get access?

A: The ITGR system is schedule to be operational NLT June 1, 2010; at which time the web address will be communicated to all agency heads, CIO's, and SAISO's.

Agency personnel must register online at the ITGR website to gain access to the system. User verification and account activation will be communicated to the user via email messages normally within 24 hours.

Q: Can I register for an ITGR system account on behalf of my commissioner or others, in my agency, who need access?

A: Yes. Go through the online registration process as you would for yourself, but enter the person's data for whom the user account is being created. The ITGR administrator will validate the user data and notify the user via email when their account is created.

Q: Do I have to use the ITGR System to do my reporting?

A: Yes. All reports must be submitted through the ITGR system. No other forms will be acceptable.

Q: Who in my agency is required to complete this report?

A: Per the Governor's executive order, the Executive Director of the agency is responsible for reporting the status of the information technology that supports their business. He/She may delegate the task of completing some or all the report to one or more personnel within that agency.

The ITGR system accommodates multiple users from a single agency to access/update their agency's report. This allows, at the discretion of the agency, different users to complete different sections of the report.

Each agency must designate one user as "***Agency Approver***" during the registration process. The Agency Approver is the only user role that can finalize and submit the completed agency ITGR. Ideally this will be the agency Executive Director; however, the Executive Director may delegate this role for another user to submit the agency ITGR on his/her behalf. This Agency Approver delegation must be communicated to GTA in writing. Please see Q&A below explaining the process.

After the agency's report is marked as "Finalized and Approved" the report will be locked and available in READ-ONLY mode and no updates can be performed.

Q: My agency's Executive Director wants me to sign off as the "Agency Approver" for the completed ITGR. Can I do that?

A: Yes. When you register on the ITGR website, select "Agency Approver" as your role in the user profile page. However, your agency executive director or commissioner must formally delegate this designation to you using the template letter below and provide the letter to GTA. The ITGR administrator will verify that the letter was received before granting you this access.

PLEASE USE OFFICIAL AGENCY STATIONERY

FAX THIS LETTER TO 404-478-9421

DATE: XX-XX-XXXX

To:
Mark Reardon
Chief Information Security and
Senior Technology Planning Officer
Georgia Technology Authority
47 Trinity Ave.
Atlanta, GA 30334

Ref: Delegation of authority to finalize and approve <Agency Name> Information Technology Governance Report

Dear Mr. Reardon:

I, <Name of Agency Commissioner>, the commissioner (or exec dir whichever applies) of <AGENCY NAME> delegate the following person to finalize and approve our Agency Information Technology Governance Report for 2010.

Name:
Title:

Regards,
name and signature of commissioner

Q: Our agency provided a lot of this information last year. Can I access last year's system data or do I have to re-enter it again?

A: Every effort is being made to reliably migrate previous year data into the new ITGR system.

Q: What is meant by the term "Enterprise"?

A: The term generally applies to an organization with common or unifying business interests and can mean different things, depending on ones perspective. For example, an enterprise may be defined at the State of Georgia level, the Sponsor level, or Business Owner level for programs and projects requiring either vertical or horizontal integration.

***For all purposes of the ITGR, consider the term to mean the State of Georgia level.*

Q: I have finished my ITGR but I cannot select the "Finalize and Approve" option in the ITGR website, why not?

A: Only a user designated as the "Agency Approver" has permissions to approve and submit the finished ITGR. By default, your commissioner (or Executive Director) has this designation. However, he/she may delegate this designation to you by providing GTA with a Delegation Letter. If this letter has been sent to GTA, contact the ITGR Administrator.

Q: My agency head or designee has locked/finalized our agency's ITGR but we need to make some changes. Can we have it unlocked?

A: Yes. Contact the ITGR Administrator for assistance.

Q: Our agency will not be able to complete the ITGR by the July 31st deadline. Can we request an extension?

A: Extension requests are not recommended but are sometimes unavoidable and will be handled on a case-by-case basis. All extension requests must be approved by the State CIO Patrick Moore. Contact the ITGR Administrator for more information.

Q: Who do I contact if I have other questions or need help with the ITGR website?

A: Please direct all ITGR system and security related questions to the ITGR Administrator, Tometrice Strickland at email ITReports@gta.ga.gov or phone 404-463-8474.

Q: Will data reported in the ITGR (e.g. system and application names) be made public?

A: While it is widely accepted within the industry that system/application names are NOT considered "sensitive" GTA will use the ITGR information to produce various State reports that may include system and application names. These reports will be provided to the Governor, Legislature and made publicly available on the ga.gov website and are also subject to open records requests. However, because the information collected via the ITGR system will continue to grow and become more detailed over time, the aggregate of that information may become sensitive. Therefore; the raw data will not be subject to open records. If you feel

that the name of your systems or applications is sensitive please use a “covert” name that is still identifiable to your agency head, CIO and the Governor’s Office.

Appendix 1: Agency Profile

Q: How do I know or where do I find my agency's Branch of Government?

A: Contact your agency head. Your agency head should have this information.

Q: How do I find out if my agency head was appointed or elected?

A: Contact your agency head. Your agency head should have this information.

Q: What/Who is a CIO?

A: An agency Chief Information Officer is the most senior executive in an organization responsible for ensuring that information technology and resources are acquired and managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and agency goals/priorities. He/she holds ultimate responsibility for the technology assets and security of information assets held by the agency.

Q: What/Who is a SAISO?

A: An agency Senior Agency Information Security Officer; formerly referred to as Agency ISO. This is the formal title (under NIST) of the primary/lead/senior person in each agency managing the information security program for that agency.

Q: Why are you asking about a Privacy Officer? Is it required?

A: A Privacy Officer is an individual within the agency with specialized expertise regarding privacy matters (both personal and professional) and whose role is to ensure awareness of data privacy issues, and compliance with regulation, legislation and policy**.** A Privacy Officer is not required. However, with the every increasing legislation and legal issues regarding privacy matters (both personal and professional), industry is recognizing the need to rely on individuals with specialized expertise in the area of privacy to focus in these matters. This question identifies those agencies that have chosen to create this function.

Q: Who/What is a BC Planner / Coordinator?

A: Business Continuity Planner or Coordinator: A role within the Business Continuity Management program that coordinates planning and implementation for business process sustainment and overall recovery of an Agency during an emergency.

Q: Who/What is a PMO?

A: Project Management Officer aka PMO Director / Manager is the individual responsible for tracking the agency projects / applications.

Q: How do I know if my agency is identified as an ESF agency?

A: ESF agencies are identified in the Governor's executive order (EO) and the Georgia Emergency Operations Plan (GEOP) as having primary and/or support responsibilities to provide essential services or support for those services during a man made, natural, or environmental state emergency.

Click this link to search the Governor's EO for Georgia Emergency Operations Plan for your agency's name.

Click here to access the Georgia Emergency Management Agency website for more information on the GEOP.

Q: How do I calculate the total number of agency employees?

A: Use the sum of the total number of filled full and part-time State employee positions as of current date and the number of active contractors employed in any capacity by the agency.

***Remember to include the employees and contractors of those agencies for which your agency has taken reporting responsibility.*

Q: I am not responsible for budget, how do I complete the questions related to Information Technology costs expended over the past Fiscal Year and budget for next fiscal year?

A: Best completed by someone in the agency finance department - Provide the expenditure totals by account code for FY2010 and the amount budgeted for these account codes for F2011.

Q: We're a GETS agency, isn't GTA (its vendors) responsible for the risk and security management of our systems?

A: No. Under GETS, GTA manages the IT service provider/s ONLY. The service provider operates and maintains the technology as directed by the system/business owners. Each GETS agency (or any agency using a service provider) always retains ownership of its business, and ultimately responsible for

ensuring the information technology adequately supports that business. Therefore, Business Owners must define the operational and security requirements for its data and ensure those requirements are being met. The service provider is responsible for meeting those requirements as requested, directed and paid for by the customer in the most efficient manner possible.

Q: We are not a GETS agency but our IT is provided by an outside third-party vendor. Are we still responsible for reporting on our IT services?

A: Yes. The same as with GETS agencies, the third party service provider operates and maintains the technology as directed by your agency. Any agency using a service provider always retains ownership of its business processes and is always responsible for ensuring adequate protection of the data and effectiveness of the technology used to support that business. Therefore, Business Owners must define the operational and security requirements for its data and ensure those requirements are being met. The service provider is responsible for meeting those requirements as requested, directed and paid for by the customer in the most efficient manner possible.

Q: How do I determine my reporting relationship with other agencies?

A: To determine your reporting relationship with other agencies, use the following definitions:
a) Self: State agencies that are responsible ONLY to themselves in the area of technology, security and risk management;
b) Self and Others: State agencies that report on their own behalf as well as for those agencies matrixed to them with a dependency to receive Information Technology services and/or risk management functions;
c) Other: State agencies that are matrixed to another agency/organization and are dependent on that agency to receive Information Technology services and/or risk management and technology reporting functions.

NOTE: All Agencies retain fiduciary responsibility for the information security of the information they own regardless of who actually operates the system on a day to day basis such as with an outsourced service provider or matrixed relationship.

Q: What is an MOU/MOA?

A: An MOU/MOA for Information Technology Services and Reporting is a written agreement between two agencies detailing the services to be performed for one agency by another. Such an agreement is required for the reporting relationships outlined in the above question.

Q: What is a Security Program?

A: A formal documented security program is an internal information security infrastructure that includes ALL of the following program elements:
a) Security management organization that assesses risk develops and implements policies, processes, and technology to adequately protect the information assets, personnel and facilities under their control and ensures compliance with Enterprise policies and standards and federal and state requirements.
b) A risk management framework
c) Internal policies and procedures
d) Business Continuity and Disaster Recovery Plan/s
e) An Incident Management and Response capability
f) Security Education and Awareness component
g) Assessment, Compliance and Enforcement mechanisms

Q: What is Information Security Governance?

A: Information Security Governance is the development, maintenance and enforcement of security policies, standards, guidelines, processes and procedures.

Click here for the Enterprise Security Policies and Standards.

Q: What is Security Categorization?

A: The level of risk (High, Moderate, or Low) that an agency poses to the State's enterprise and/or their constituency for the security objectives of Confidentiality, Integrity, and Availability. Agencies are categorized based on the highest impact rating (high water mark) assigned to any operational/production system which should also be equal to the highest impact rating assigned to any application running on that system:
High - High Impact is the system or application categorization assigned if, for ANY security objective, the potential for loss of life, severe or catastrophic adverse effect on organizational operations, assets or individuals.
Moderate - Moderate Impact is the system or application categorization assigned if, for ANY security objective, the potential for serious adverse effect on organizational operations, assets, or individuals.
Low - Low Impact is system/application categorization assigned if, for ALL security objectives, the potential for limited or minimal adverse effect on organizational operations, assets, or individuals

Q: What do you mean by "Readily Available"?

A: "Readily Available" means accessible by employees easily at any time.

Q: When asked about "How many agency employees completed annual security awareness training" do you mean how many completed annual training this year?

A: Yes. Security awareness training is required to be completed every year (annually) by every employee.

Q: Is there a new/updated security awareness video or can we reuse the security awareness video from GTA from last year?

A: The GTA security awareness video was updated this year (Please DO NOT use any previous version of the video). The security awareness video that GTA published meets the general user annual requirement and therefore, agencies are welcome to use this video or you may use other material as your agency sees appropriate.

To obtain a copy please contact Walter Tong via email: walter.tong@gta.ga.gov or phone: 404-651-9754.

Q: What is Business Continuity Planning?

A: Process of developing and documenting triggers, people, communications and procedures that enable an agency to respond to an event that lasts for an unacceptable period of time and return to performing its critical business functions after an interruption.

Q: What is a Business Continuity Plan?

A: The resulting BC planning document that details the processes and procedures required to enable an Agency to respond to an event that lasts for an unacceptable period of time and resume performing its critical business functions after an interruption.

Q: Is a Business Process the same as a business plan?

A: A "business process" is owned and carried out by the business side of the agency, not the IT department, although a business process may depend upon the IT department. An agency business process contributes to the delivery of a product or service to the agency clients. For example, the Department of Revenue needs a methodology to receive, deposit and account for tax revenues in order to deliver services to their business customers the taxpayers. "Core" business processes are absolutely required to accomplish business.

Q: What is LDRPS?

A: LDRPS is a tool provided by GTA to agencies for documenting BC plans.

Q: What is a Security Incident Response Plan?

A: A Security Incident Response Plan is your agency's methodology for preventing, monitoring, detecting, containing, responding, recovering, reporting and escalating threats or violations of security policy and/or controls and limiting their affects to the organization. See Enterprise PSG: SS-08-004 Incident Response and Reporting Standard

Q: Does my agency have to have a documented Security Incident Management Plan?

A: Yes, see Enterprise PSG: SS-08-004 Incident Response and Reporting Standard

Q: What is a "legitimate" security issue?

A: A legitimate security issue is associated with any incident that upon examination is determined to be an inadvertent or an intentional breach or violation of management, operational and/or technical security policies.

Appendix 2: Production System Inventory

Q: Explain what you classify as a "system"?

A: A system is a discrete set of information resources (workstations, servers, minor applications, network, etc) working together for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

NOTE: For the purposes of the State IT Governance Report, only Production systems are reported (not major business applications within the system boundaries).

Production systems are those IT systems that are readily available, in use and actively supporting the business. It is common in the industry to call these systems "Operational Systems". Production systems do not include research, development or test systems.

Q: Why do I have to document the characteristics of all my systems?

A: To effectively run and improve a business, the business must understand the risks. To understand the risks and effectively mitigate them, the business must know what it has, how it uses it and what it needs. To know this and make crucial business decisions, systems must be fully and accurately documented.

Q: What are the Security Objectives?

A: The goals of security controls within in an IT environment. The objectives are:
Confidentiality - to prevent unauthorized disclosure of information
Integrity - to prevent unauthorized modification, destruction or disputable authenticity of information
Availability - to prevent disruption of access or use of information or an information system

Q: What is an Information System Security Plan?

A: System Security plans are living documents that are developed, reviewed and updated throughout the systems lifecycle to accurately reflect the current state of the information system. See Enterprise PSG: SS-08-028.01 System Security Plans Standard.

Q: What is a FISMA-based security assessment?

A: A FISMA-based assessment of system or application security controls is based on the FISMA risk management framework and NIST SP800-53. (The Federal Information Security Management Act formed the basis of the National Institute of Standards for Technology reference SP800-53, which is endorsed and adopted by GTA for security management)

Required by Enterprise PSG SS-08-042.01, Independent Security Assessments Standard.

Q: Who is the Business Owner?

A: The Business Owner is ultimately responsible for ensuring appropriate confidentiality, integrity, and availability of IT systems and information needed to support the business. He/she must be fully aware of the risks associated with operating an information system or application that supports his/her business area and has taken the necessary steps to either mitigate those risks or accept them. See Enterprise Standards:
SA-10-001.01 Placing Applications into Production.

Q: What is a Disaster Recovery Plan (DRP)?

A: A disaster recovery plan is an element of BC Planning that documents the processes and procedures to identify, to prioritize and to restore the IT operations which support business following an interruption.

Q: Who is the service provider?

A: The State's Enterprise Operating Vendors are those who operate GETS (IBM and AT&T).

Q: How do I calculate agency FTEs?

A: FTE - Full Time Equivalent State employees is a calculated figure to indicate the proportion of full time labor applied to a given task. Is calculated as follows:

Calculate FTE for State employee positions
- A staff position applied full-time in support = 1.0 FTE
- If a portion of the position is applied in support (say 10%) = 1.0 x .10 = .10 FTE
- If 5 staff positions each spend 30% in support = 5 x .30 = 1.50 FTE

• If part-time hourly position works 500 hours annually and spends 10% of that supporting this application, the FTE calculation is: 500 x .10 divided by 2080 = .02 FTE (rounded).

Q: How do I calculate contractor FTEs?

A: FTE - Full Time Equivalent Contractor employees
A calculated figure to indicate the proportion of full time labor applied to a given task. Is calculated as follows:

Calculate FTE for Contractor employee positions
• A contractor position applied full-time in support = 1.0 FTE
• If a portion of a contractor position is applied in support (say 10%) = 1.0 x .10 = .10 FTE
• If 5 contractor positions each spend 30% in support = 5 x .30 = 1.50 FTE
divide hours applied (say 500) by 2080 (the hourly equivalent of working full time) = 500/2080 = .0
• If part-time hourly contractor works 500 hours annually and spends 10% of that supporting this application, the FTE calculation is: 500 x .10 divided by 2080 = .02 FTE (rounded)

Appendix 3: Business Application Inventory

Q: Explain what you classify as a "business application"?

A: An application is a set of computer programs related to a business function which allows the business to achieve operational goals.

Q: Who is an Application Business Owner?

A: The Business Owner is an individual stakeholder (usually an executive) who serves as the primary customer and advocate for the applications and technology that support their business functions and that establishes and funds the agency's/business units' strategic objectives.

Q: What is a subprogram?

A: For budgeting purposes an agency is divided into "programs" based on its strategic goals and objectives. If necessary these programs are subdivided based on more specific strategic goals and objectives into "subprograms". These program and subprograms have associated budgets. Business applications support 1 or more programs and/or subprograms within an agency. For each application, provide the name/s of the program/s and/or subprogram/s that are supported by this application

Q: What is a Program Code (PeopleSoft Financial Code)?

A: The General Ledger designation used to track expenditures for the program.

Q: How essential is this application to the agency's core business?

A: *Critical* - Agency goals would not be met if application did not function.
Important - The agency could operate but may not meet its critical goals if the application did not function.
Supportive - The application only supports basic agency functions and is not necessary to achieve goals.

Q: What is an Application Security Plan?

A: An application security plan is an application specific section of the system security plan

Q: Who is the Application Business Owner?

A: The Business Owner is the individual ultimately responsible for ensuring appropriate confidentiality, integrity, and availability of IT systems and information needed to support the business. He/she must be fully aware of the risks associated with operating an information system or application that supports his/her business area and has taken the necessary steps to either mitigate those risks or accept them. See Enterprise Standard SA-10-001.01 at Placing Applications into Production Standard

Q: What is the Platform and operating system hosting the application?

A: Platform" is the type of computing hardware the application is running on. "Operating" System is the core system software running on a hardware platform.

Q: Are you asking whether or not a customer satisfaction survey was conducted on our applications during this fiscal year?

A: Yes. Answer NO if the survey was done prior to FY 2010.

Appendix 4: Project Portfolio

Q: What is a Project?

A: A project is a temporary endeavor that delivers business objectives.

Q. What is a Stage Gate Review?

A. The last task of each phase in the EPLC is a Stage Gate Review to ensure that the investment status may progress to the next phase. Stage Gate Reviews consist of an independent confirmation by Critical Partners to the IT governance organization that the Project Manager has satisfactorily produced all the required deliverables and adequately met all exit criteria for the phase to permit advancement to the next phase. The emphasis of Stage Gate Reviews is on:
- The successful accomplishment of the phase objectives.
- The plans for the next life cycle phase.
- The risks associated with moving into the next life cycle phase.

See http://www.gta.ga.gov : Enterprise Program and Project Management Office page - Enterprise Performance Lifecycle

Q: What is the Enterprise Performance Life Cycle (EPLC)?

A: A methodology to organize the activities, deliverables, and governance reviews activities of project managers and all stakeholders during the life of an IT investment into ten life-cycle phases. Seven of the ten phases are traditional "project" lifecycle phases; the remaining phases are investment phases of conception, operation and disposal of the IT investment. The phases are:
1) concept 2) initiation 3) planning 4) requirements analysis 5) design 6) development 7) test 8) transition 9) operations 10) dispose.
The last step of each phase is a Stage Gate Review to ensure that the investment status may progress to the next phase.

See http://www.gta.ga.gov : Enterprise Program and Project Management Office - Enterprise Performance Lifecycle

Q: How is agency SAISOs or other IT professionals supposed to know the answers to these IT expenditure questions?

A: Although we have consolidated the reporting mechanisms, the required reporting information will not likely come from a single source within the agency. The ITGR website supports multiple users with an agency. Please direct the various sections of the report to the appropriate business units or personnel within

your agency. Whoever from your agency completed the IT Expenditures Report in past years will likely be the source to complete it this year. The only difference is the delivery format and reporting tool.

Q: Explain what is meant by expenditures for a project?

A: A Project is defined as those IT related aspects of a business goal that will cost more than $100,000. Project expenditures are all costs incurred during the current reporting year including FTE salaries. A subset of costs incurred for some projects are from non-state issued sources. Finally, there is a lifecycle for all projects that should have estimated costs projected for its analysis, development, implementation, operations, maintenance and eventual decommissioning including FTE salaries.

Q: Who do I contact if I have questions or need help with expenditure information?

A: Direct IT Expenditures questions to: Tom Fruman at email tfruman@gta.ga.gov or phone 404-463-6815